

WHAT IS CLAIMED IS:

1. A system for evaluating M modulo J, where J is an integer and M is an integer
 2 expressed in binary form ($M = \sum_{i=0}^N \alpha_i 2^i$), where α_i is 0 or 1, and $N+1$ is the number of
 digits in a binary word) comprising:
 - 4 a first circuit for decomposing M into two integers A and $B = M - A$;
 - a second circuit for evaluating (A modulo J);
 - 6 a third circuit for evaluating $M' = (A \text{ modulo } J) + B$; and
 - a fourth circuit for outputting M' or feeding M' back to the first means to
 8 evaluate M' modulo J.
2. The system of Claim 1, wherein the first circuit includes a multiplexer M1
 2 which passes $B_N = (M - \alpha_N 2^N)$ to the second circuit on a first iteration, and passes $B_i =$
 $(M' - \alpha_i 2^i)$ on all subsequent iterations, where i is an iteration counter starting with N and
 4 counting down.
3. The system of Claim 1, wherein the second circuit includes a look-up table
 2 that stores $C_i = 2^i \text{ modulo } J$ for $i = 0$ to N.
4. The system of Claim 3, wherein the second circuit further includes a
 2 multiplexer M2 that passes 0 to the third circuit when ($\alpha_i = 0$), and passes C_i when ($\alpha_i =$
 1).

5. The system of Claim 1, wherein the third circuit includes an adder A1 whose
2 inputs are B_i and $(\alpha_i C_i)$ and which passes its output $M' = B_i + (\alpha_i C_i)$ to the fourth circuit.

6. The system of Claim 1, wherein the fourth circuit includes a multiplexer M4
2 that passes M' as a final output if $(M' < J)$; otherwise i is set to $i-1$, and M' is fed back to
the first circuit.

7. The system of Claim 1, wherein the circuit further includes fifth circuit for
2 ensuring convergence.

8. The system of Claim 7, wherein the fifth circuit includes a multiplexer M3
2 that passes J when the bitwise AND of M' and J equals J , otherwise it passes 0.

9. The system of Claim 8, wherein the output of the multiplexer M3 is subtracted
2 from M' by an adder A2 and the result is passed to the fourth circuit.

10. A deinterleaver comprising:

2 a demultiplexer;

a multiplexer; and

4 a circuit for connecting the outputs of the demultiplexer to the inputs of the
multiplexer, wherein the circuit includes a system for evaluating M modulo J

6 comprising:

EL903006554 US

- a first circuit for decomposing M into two integers A and $B = M - A$;
- 8 a second circuit for evaluating $(A \text{ modulo } J)$;
- a third circuit for evaluating $M' = (A \text{ modulo } J) + B$; and
- 10 a fourth circuit for outputting M' or feeding M' back to the first circuit to evaluate $M' \text{ modulo } J$.

11. A method for evaluating $M \text{ modulo } J$ including the steps of:

- 2 decomposing M into two integers A and $B = M - A$;
- evaluating $(A \text{ modulo } J)$;
- 4 evaluating $M' = (A \text{ modulo } J) + B$; and,
- determining whether to output M' as the final answer, or to feedback M' to the
- 6 decomposing step to evaluate $M' \text{ modulo } J$.

- 12. The method of Claim 11, wherein the decomposing involves passing $B_N =$
- 2 $(M - \alpha_N 2^N)$ to the evaluating $(A \text{ modulo } J)$ step on a first iteration, and passing $B_i = (M' - \alpha_i 2^i)$ on all subsequent iterations, where i is an iteration counter starting with N and
- 4 counting down.

- 13. The method of Claim 11, wherein evaluating $(A \text{ modulo } J)$ involves using a
- 2 look-up table that stores $C_i = 2^i \text{ modulo } J$ for $i = 0$ to N .

14. The method of Claim 13, wherein the evaluating $(A \text{ modulo } J)$ further

EL903006554 US

- 2 includes passing 0 to the evaluating $M' = (A \text{ modulo } J) + B$ step when $(\alpha_i = 0)$, and passes C_i when $(\alpha_i = 1)$.

15. The method of Claim 11, wherein the evaluating $M' = (A \text{ modulo } J) + B$ step

- 2 involves using an adder A1 whose inputs are B_i and $(\alpha_i C_i)$ and which passes its output $M' = B_i + (\alpha_i C_i)$ to the determining step.

16. The method of Claim 11, wherein the determining involves passing M' as a

- 2 final output when $(M' < J)$; otherwise i is set to $i-1$, and M' is fed back to the decomposing step.

17. The method of Claim 12, further comprising ensuring convergence has

- 2 occurred.

18. The method of Claim 17, wherein ensuring convergence includes passes J

- 2 when the bitwise AND of M' and J equals J , otherwise passing 0.